Cassandra Crossing/ Colpevoli di Ransomware

(475)—Non esistono giustificazioni per chi offre servizi e viene colpito da ransomware

---

Cassandra Crossing/ Colpevoli di Ransomware
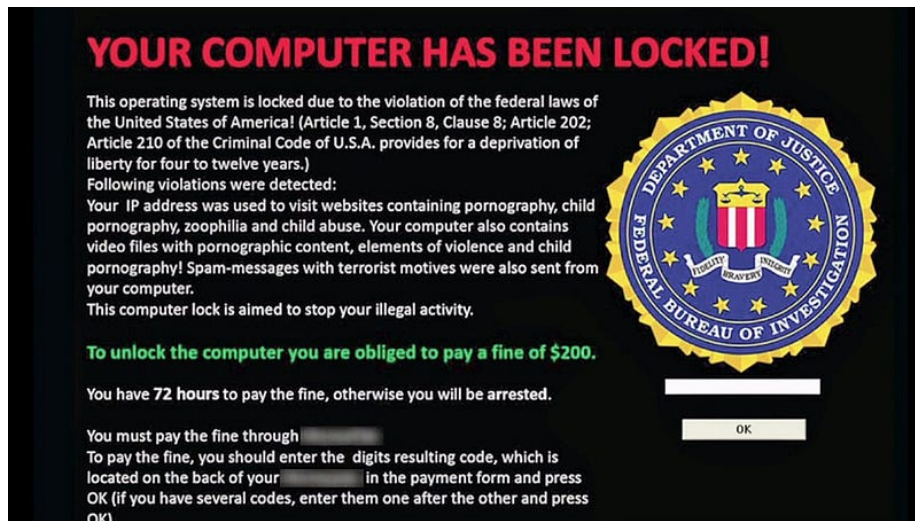
Figure 1: https://commons.wikimedia.org/wiki/File:Ransomware-pic.jpg

(475)—Non esistono giustificazioni per chi offre servizi e viene colpito da ransomware

15 aprile 2021—Esiste una importante astrazione legale; la "*Cura del buon padre di famiglia*".

E' il livello di attenzione che chiunque svolga un'attività, particolarmente se diretta al pubblico, deve mantenere per non essere colpevole di negligenza, e quindi automaticamente soccombente in un giudizio civile per danni.

La "*Cura del buon padre di famiglia*" viene valutata di volta in volta, in relazione al mercato ed alle tecnologie disponibili al momento del fatto.
Valutazione molto difficile? Può darsi, ma **in ambito legale viene eseguita assai frequentemente**.

Alcuni soggetti particolari, come ad esempio gli iscritti ad albi professionali, sono invece tenuti, nell'esecuzione del loro lavoro, a livelli di attenzione molto superiori alla normale "Cura del buon padre di famiglia".
Per loro non basta la "Cura" normale per essere incolpevoli in caso di problemi.

Cassandra, che non ama particolarmente le astrazioni legali, è stata costretta a questa lunga introduzione per formulare la sua tesi.

Si, perché non della solita profezia si tratta, ma di un'invocazione.

Nel 2021 è ahimè ancora possibile che un utente di servizi cloud o di hosting di server fisici perda dati per colpa di un incendio.
Non dovrebbe succedere ma può succedere, e non è facile impedirlo.

Ma oggi è inammissibile che qualcuno perda dati a causa di un ransomware. Nessun fornitore di servizi, nessuna rete aziendale che offra servizi a terzi, può nel 2021 perdere dati a causa di un ransomware.

Un ransomware può bloccare un'intera rete aziendale, se gestita male, e può anche bloccare l'erogazione di servizi per un po' di tempo, ma è inammissibile che non esistano backup dei dati, o che anche i backup vengano criptati dal ransomware.

I backup "*offline*", garantiti a prova di qualsiasi ransomware, presente o futuro, sono elementari ed economici.
Li si può fare in tutte le situazioni ed in qualsiasi sistema informatico, in mille modi diversi, da quelle casalinghi, fatti con un disco USB da 50 euro (anzi due), fino ai più esoterici e complessi.

Le organizzazioni che perdono dati di altri per colpa di un ransomware dovrebbero essere, per questo solo fatto, automaticamente considerate colpevoli, avendo evidentemente operato ad un livello qualitativo incredibilmente più basso della "Cura del buon padre di famiglia".

Un po' di storia recente.

Nel 2017 il colosso della logistica Maersk è stata bloccata per due settimane, incapace di fornire il servizio di trasposto container ad una percentuale significativa del traffico merci mondiale, con perdite immediate stimate in centinaia di milioni di dollari e conseguenze devastanti, sia sulle quotazioni azionarie che per la bile dei propri clienti, e dei loro autisti e marinai.

Anche se la notizia non ha fatto molto scalpore nei media "ordinari", per ben due settimane i maggiori porti di tutto il mondo sono stati intasati dai Tir bloccati, che non sapevano dove scaricare o caricare i loro container, e centinaia di migliaia di container erano irrintracciabili in giro per mondo, accatastati nei porti, sui Tir o sulle navi portacontainer.

Era il 2017, ed il ransomware NotPetya, con un'unica infezione, mise in ginocchio il mondo del trasporto merci. E le conseguenze, bene elencate qui sarebbero potute essere ancora peggiori se un server ActiveDirectory secondario in un'oscura filiale africana della Maersk non fosse stato offline per un guasto, conservando così una copia non criptata dei dati.

Un "backup offline" del tutto casuale ed involontario, che ha permesso così di "risparmiare" la ricostruzione da zero della configurazione dell'intera rete

aziendale globale.

Ma da allora, in molti, troppi altri posti, non molto è cambiato.

Intere reti aziendali di multinazionali, di ospedali e di utilities continuano ad essere vittima di ransomware che, oltre all'inevitabile ma temporanea interruzione di servizi, provocano spesso anche la perdita di dati.

E perdere dati in questo modo, quando sono importanti o li si gestisce per altri, non è più ammissibile.

Dopo 4 anni dal caso Maersk la lezione deve essere stata bene imparata da tutti; niente di tutto ciò deve più accadere.
Se accade, l'**essere vittima di un ransomware deve essere considerato una colpa grave per mancanza della "Cura del buon padre di famiglia"**.

Eppure i ransomware continuano a colpire, e i dirigenti delle aziende colpite a cercare rifugio dietro fumose "policy aziendali". E qualcuno ci crede!

Manca ancora la "ciccia", il rispetto pratico di standard minimi di sicurezza, mancano i soldi spesi per la sicurezza dei sistemi informativi, soldi che devono essere visti non come uno spreco ma come una polizza sulla vita.

Parlate oggi di policy ad un impiegato della Maersk e vi zittirà; **da loro è diventata una parola vietata**.

By Marco A. L. Calamari on April 13, 2021.

Canonical link

Exported from Medium on January 2, 2024.